NASA Procedural Requirements

NPR 8705.4
Effective Date: June 14, 2004
Expiration Date: June 14, 2009

COMPLIANCE IS MANDATORY

Printable Format (PDF)

Subject: Risk Classification for NASA Payloads

Responsible Office: Office of Safety and Mission Assurance

Appendix B - Recommended SMA-Related Program Requirements for NASA Class A-D Payloads

	CLASS A	CLASS B	CLASS C	CLASS D
Single Point Failures (SPFs)	Critical SPFs (for Level 1 requirements) are not permitted unless authorized by formal waiver. Waiver approval of critical SPFs requires justification based on risk analysis and implementation of measures to mitigate risk.	Critical SPFs (for Level 1 requirements) may be permitted but are minimized and mitigated by use of high reliability parts and additional testing. Essential spacecraft functions and key instruments are typically fully redundant. Other hardware has partial redundancy and/or provisions for graceful degradation.	Critical SPFs (for Level 1 requirements) may be permitted but are mitigated by use of high reliability parts, additional testing, or by other means. Single string and selectively redundant design approaches may be used.	Same as Class C.
Engineering Model, Prototype, Flight, and Spare Hardware	Engineering model hardware for new or modified designs. Separate prototype and flight model hardware. Full set of assembled and tested "flight spare" replacement units.	Engineering model hardware for new or significantly modified designs. Protoflight hardware (in lieu of separate prototype and flight models) except where extensive qualification testing is anticipated. Spare (or refurbishable prototype) hardware as needed to avoid major program impact.	Engineering model hardware for new designs. Protoflight hardware permitted (in lieu of separate prototype and flight models). Limited flight spare hardware (for long lead flight units).	Limited engineering model and flight spare hardware.
Qualification, Acceptance, and Protoflight Test Program	Full formal qualification and acceptance test programs and integrated end-to-end testing at all hardware and software levels.	Formal qualification and acceptance test programs and integrated end-to-end testing at all hardware levels. May use a combination of qualification and protoflight hardware. Qualified software simulators used to verify software and system.	Limited qualification testing for new aspects of the design plus full acceptance test program. Testing required for verification of safety compliance and interface compatibility.	Testing required only for verification of safety compliance and interface compatibility. Acceptance test program for critical performance parameters.
EEE Parts *http: // nepp .nasa .gov/ index_nasa .cfm/ 641	NASA Parts Selection List (NPSL)* Level 1, Level 1 equivalent Source Control Drawings (SCDs), and/or requirements per Center Parts Management Plan.	Class A requirements or NPSL Level 2, Level 2 equivalent SCDs, and/or requirements per Center Parts Management Plan.	Class A, Class B or NPSL Level 3, Level 3 equivalent SCDs, and/or requirements per Center Parts Management Plan.	Class A, Class B, or Class C requirements, and/or requirements per Center Parts Management Plan.

Reviews	Full formal review program.Either IPAO external independent reviews or independent reviews managed at the Center level with Enterprise Office participation. Include formal inspections of software requirements, design, verification documents, and code.	Full formal review program.Either IPAO external independent reviews or independent reviews managed at the Center level with Enterprise Office participation. Include formal inspections of software requirements, design, verification documents, and peer reviews of code.	Full formal review program. Independent reviews managed at Center level with Enterprise Office participation. Include formal inspections of software requirements, peer reviews of design and code.	Center level reviews with participation of all applicable directorates. May be delegated to Projects. Peer reviews of software requirements and code.
Safety* NPD 8700.1	Per all applicable NASA safety standards.	Same as Class A.	Same as Class A.	Same as Class A.
Materials	Verify heritage of previously used materials and qualify all new or changed materials and applications/configurations. Use source controls on procured materials and acceptance test each lot/batch.	Use previously tested/flown materials or qualify new materials and applications/configurations. Acceptance test each lot of procured materials.	Use previously tested/flown materials or characterize new materials. Acceptance test sample lots of procured materials.	Requirements are based on applicable safety standards. Materials should be assessed for application and life limits.
Mishap Investigation Board Requirements *NPR 8621.1	Initiated and conducted per NPR 8621.1.	Initiated and conducted per NPR 8621.1.	Initiated and conducted per NPR 8621.1.	Initiated and conducted per NPR 8621.1.
Reliability *NPD 8720.1	Failure mode and effects analysis/critical items list (FMEA/CIL), worst-case performance, and parts electrical stress analysis for all parts and circuits. Mechanical reliability, human, and other reliability analysis where appropriate.	FMEA/CIL at black box (or circuit block diagram) level as a minimum. Worst-case performance and parts electrical stress analysis for all parts and circuits.	FMEA/CIL scope determined at the project level. Analysis of interfaces. Parts electrical stress analysis for all parts and circuits.	Analysis requirements based on applicable safety requirements. Analysis of interface.
Reliability *NPD 8720.1	Failure mode and effects analysis/critical items list (FMEA/CIL), worst-case performance, and parts electrical stress analysis for all parts and circuits. Mechanical reliability, human, and other reliability analysis where appropriate.	FMEA/CIL at black box (or circuit block diagram) level as a minimum. Worst-case performance and parts electrical stress analysis for all parts and circuits.	FMEA/CIL scope determined at the project level. Analysis of interfaces. Parts electrical stress analysis for all parts and circuits.	Analysis requirements based on applicable safety requirements. Analysis of interface.
Fault Tree Analysis	System level qualitative fault tree analysis.	Same as Class A.	Same as Class A.	Fault tree analysis required for safety critical functions.
Probabilistic Risk Assessment *NPR 8705.xx	Full Scope, addressing all applicable end states per NPR 8705.xx.	Limited Scope, focusing on mission-related end-states of specific decision making interest per NPR 8705.xx.	Simplified, identifying major mission risk contributors.Other discretionary applications.	Safety only.Other discretionary applications.
Maintainability[1] *NPD 8720.1	As required by NPD 8720.1	Application of NPD 8720.1 determined by program. (Typically ground elements only.)	Maintainability considered during design if applicable.	Requirements based on applicable safety standards.
Quality Assurance *NPD 8730.3 * NPR 8735.2 * NPD 1280.1 (NPR 8735.1A)	Formal quality assurance program including closed-loop problem reporting and corrective action, configuration management, performance trending, and stringent surveillance. GIDEP failure experience data and NASA Advisory process.	Formal quality assurance program including closed-loop problem reporting and corrective action, configuration management, performance trending, moderate surveillance. GIDEP failure experience data and NASA Advisory process.	Formal quality assurance program including closed-loop problem reporting and corrective action, configuration management, tailored surveillance. GIDEP failure experience data and NASA Advisory process.	Closed-loop problem reporting and corrective action, configuration management, GIDEP failure experience data and NASA Advisory process. Other requirements based on applicable safety standards.
Software *NPD 8730.4	Formal project software assurance program. Independent Verification and Validation (IV&V) as determined by AA OSMA.	Formal project software assurance program. IV&V as determined by AA OSMA.	Formal project software assurance program. IV&V as determined by AA OSMA.	Formal project software assurance insight. IV&V as determined by AA OSMA.
Risk Management *NPR 7120.5	Risk Management Program. Risk reporting to GPMC.	Same as Class A.	Same as Class A.	Same as Class A.
Telemetry Coverage	During all mission critical events to assure data is available for critical anomaly investigations to prevent future recurrence.	Same as Class A.	Same as Class A.	Same as Class A.

[1]For ISS payloads, maintainability, reliability, and availability requirements should be defined at an early phase and plans addressed during the design, development, and testing of the payload, regardless of class. Components with low reliability should be assessed for on-orbit maintainability based on the availability requirements, and other relevant factors. The balance of these factors should result in a payload that meets performance requirements for the required duration of flight.

| TOC | Preface | Chapter1 | Chapter2 | AppendixA | AppendixB | AppendixC | ALL |

| NODIS Library | Program Management(8000s) | Search |

DISTRIBUTION:
NODIS
